

Notice of Allowability

Application No.

10/679,879

Examiner

Randal D. Moran

Applicant(s)

TANAKA ET AL.

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 7/20/2007.
2. ☒ The allowed claim(s) is/are 1-17.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
 - * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

/RDM/

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Joseph Price on 10/15/2007.

The application has been amended as follows:

1. (currently amended) A particular plaintext detector for detecting whether each of a plurality of plaintexts to be inputted into a predetermined encryption algorithm satisfies a predetermined condition, the particular plaintext detector comprising:

a receiving part [[for]] receiving the plurality of plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number.

2. (currently amended) A particular plaintext detector for detecting whether each of a plurality of plaintexts, to be inputted into a block encryption algorithm, satisfies a predetermined condition, the block encryption algorithm receiving and stirring each of the plurality of plaintexts with a key step by step to perform encryption and outputting ciphertext, the particular plaintext detector comprising:

a receiving part [[for]] receiving the plurality of plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting

Art Unit: 2135

the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number.

3. (currently amended) A particular plaintext detector for detecting whether each of a plurality of plaintexts to be inputted into a KASUMI type encryption algorithm having a stirring step satisfies a predetermined condition, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives the plurality of plaintexts sequentially, has a plurality of stirring steps for stirring with a key, and performs encryption step by step to output ciphertext, the particular plaintext detector comprising:

a receiving part [[for]] receiving the plurality of plaintexts sequentially;

a counter part [[for]] separating 17th to 32nd bits of each of the plurality of plaintexts into a fixed part and 1st to 16th bits and 33rd to 64th bith thereof into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing it as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number.

4. (currently amended) A filter apparatus for limiting an output of ciphertext from an encryption algorithm that receives a plurality of plaintexts and outputs ciphertext, the filter apparatus comprising:

- a receiving part [[for]] receiving the plurality of plaintexts sequentially;
- a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing it as a separate count; and

- a detecting part [[for]] outputting a detection signal when at least one of the separate counts exceeds a predetermined number; and

- a filter apparatus main body [[for]] outputting each of the plaintext when a detection signal is not outputted from the detecting part, and for holding the further output of each of the plurality of plaintexts until it receives a process restart signal for instructing a restart of outputting each of the plurality of plaintext when the detection signal that shows the encryption algorithm is susceptible to a decryption attack is outputted.

5. (currently amended) An encryption apparatus for executing an encryption algorithm that receives each of a plurality of plaintexts to output ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

- a receiving part [[for]] receiving the plurality of the plaintexts sequentially;
- a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting

Art Unit: 2135

the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number;

an encryption apparatus main body [[for]] performing the encryption algorithm for encryption of those plurality of plaintexts subject to the detecting part and the detection signal is not outputted from the detecting part, and for holding output of any plurality of plaintexts when the detection signal is outputted; an indication signal receiving part [[for]] receiving an indication signal for indicating a change in the encryption algorithm for subsequent encryption; and

a setting part [[for]] outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information required for setting information corresponding to the encryption algorithm for the fixed part and the set of the values of the fixed parts and used by the counter part based on the indication signal,

wherein the encryption apparatus main body and the counter part perform the settings based on the cipher setting information and the counter part setting information.

6. (currently amended) An encryption apparatus for executing an encryption algorithm that receives a plurality of plaintexts to calculate ciphertext with a key, the encryption apparatus comprising:

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number; and

an encryption apparatus main body [[for]] updating the key used for encryption when a detection signal is outputted from the detecting part.

7. (currently amended) A ciphertext storing apparatus for executing an encryption algorithm that receives a plurality of plaintexts to calculate ciphertext with a key, and storing the ciphertext, the ciphertext storing apparatus comprising:

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number; and

a ciphertext storing part allowed to store ciphertext; and

a ciphertext storing apparatus main body [[for]] updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing partially each of the plaintexts, the ciphertext, and key reference information allowing reference of the key having been used for encryption in the ciphertext storing part.

8. (currently amended) A filter apparatus for limiting output of ciphertext from a block encryption algorithm that receives and stirs each of a plurality of plaintexts with a key step by step to perform encryption and outputs ciphertext, the filter apparatus comprising:

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number; and

a filter apparatus main body [[for]] outputting each of the plaintext when a detection signal is not outputted from the detecting part, and for holding an output of each of the plurality of plaintexts until it receives a process restart signal for instructing a restart of outputting each of the held plurality of plaintext when the detection signal is outputted.

9. (currently amended) An encryption apparatus for executing a block encryption algorithm that receives and stirs each of the plurality of plaintexts with a key, step by step, to perform encryption and outputs ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising;

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number; and

an encryption apparatus main body [[for]] executing the encryption algorithm for encryption when a detection signal is not outputted from the detecting part, and for holding output of each of the plurality of plaintexts when the detection signal is outputted;

an indication signal receiving part [[for]] receiving an indication signal for indicating a change in the encryption algorithm for subsequent encryption; and

a setting part [[for]] outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information for setting information corresponding to the encryption algorithm for

the fixed part and the set of values of the fixed parts and used by the counter based on the indication signal,

wherein the encryption apparatus main body and the counter part perform the settings based on the ciphertext setting information and the counter part setting information.

10. (currently amended) An encryption apparatus for executing a block encryption algorithm that receives and stirs each of a plurality of plaintexts with a key, step by step, to perform encryption and outputs ciphertext, the encryption apparatus comprising:

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count; and

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number; and

an encryption apparatus main body [[for]] updating the key used for encryption when a detection signal is outputted from the detecting part.

11. (currently amended) A ciphertext storing apparatus for executing a block encryption algorithm that receives and stirs each of a plurality of plaintexts with a key, step by step, to perform encryption and outputs ciphertext, and storing the ciphertext, the ciphertext storing apparatus comprising:

Art Unit: 2135

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating a predetermined part from a bit string forming each of the plaintexts into a fixed part and a remaining part into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing the number as a separate count;

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number;

a ciphertext storing part storing ciphertext; and

a ciphertext storing apparatus main body [[for]] updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing partially each of the plaintexts, the ciphertext, and key reference information allowing reference of the key having been used for encryption in the ciphertext storing part.

12. (currently amended) A filter apparatus for limiting an output of ciphertext from a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives a plurality of plaintexts sequentially, has a plurality of stirring steps for [[stir]] stirring with a key, and performs encryption step by step to output ciphertext, the filter apparatus comprising:

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating 17th to 32nd bits of each of the plurality of plaintexts into a fixed part and 1st to 16th bits and 33rd to 64th bits thereof into a variable

Art Unit: 2135

part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part ~~[[for]]~~ outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number; and

a filter apparatus main body ~~[[for]]~~ outputting each of the plaintext when a detection signal is not outputted from the detecting part, and for holding the further output of each of the plurality of plaintexts until it receives a process restart signal for instructing a restart of outputting each of the held plurality of plaintext when the detection signal is outputted.

13. (currently amended) An encryption apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives a plurality of plaintexts sequentially, has a plurality of stirring steps for ~~[[stir]]~~ stirring with a key, and performs encryption step by step to output ciphertext in which the encryption algorithm is changeable, the encryption apparatus comprising:

a receiving part ~~[[for]]~~ receiving the plurality of the plaintexts sequentially;

a counter part ~~[[for]]~~ separating 17th to 32nd bits of each of the plurality of plaintexts into a fixed part and 1st to 16th bits and 33rd to 64th bith thereof into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number;

an encryption apparatus main body [[for]] executing the encryption algorithm for encryption of those plurality of plaintexts subject to the detecting part and the detection signal is not outputted from the detecting part, and for holding an output of each of the plurality of plaintexts when the detection signal is outputted,

an indication signal receiving part [[for]] receiving an indication signal for indicating a change in the encryption algorithm for subsequent encryption; and

a setting part [[for]] outputting cipher setting information required for setting the encryption algorithm executed by the encryption apparatus main body and counter part setting information corresponding to the encryption algorithm for the fixed part and used by the counter part based on the indication signal,

wherein the encryption apparatus main body and the counter part perform the settings based on the ciphertext setting information and the counter part setting information.

14. (currently amended) An encryption apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives a plurality of plaintexts sequentially, has a plurality of stirring steps for [[stir]] stirring with a key, and performs encryption step by step to output ciphertext, the encryption apparatus comprising:

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating 17th to 32nd bits of each of the plurality of plaintexts into a fixed part and 1st to 16th bits and 33rd to 64th bith thereof into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number;

an encryption apparatus main body [[for]] updating the key used for encryption when a detection signal is outputted from the detecting part.

15. (currently amended) A ciphertext storing apparatus for executing a KASUMI type encryption algorithm having a stirring step, the KASUMI type encryption algorithm equal to KASUMI which is a block encryption algorithm that receives a plurality of plaintexts sequentially, has a plurality of stirring steps for [[stir]] stirring with a key, and performs encryption step by step to output ciphertext, and storing the ciphertext, the ciphertext storing apparatus comprising:

a receiving part [[for]] receiving the plurality of the plaintexts sequentially;

a counter part [[for]] separating 17th to 32nd bits of each of the plurality of plaintexts into a fixed part and 1st to 16th bits and 33rd to 64th bith thereof into a variable part, counting the number of inputted plaintexts each of which has the same value of the fixed part, and storing it as a separate count;

a detecting part [[for]] outputting a detection signal that shows the encryption algorithm is susceptible to decryption attack when at least one of the separate counts exceeds a predetermined number;

a ciphertext storing part allowed to store ciphertext; and

a ciphertext storing apparatus main body [[for]] updating the key used for encryption when a detection signal is outputted from the detecting part, and for storing partially each of the plaintexts, the ciphertext, and key reference information allowing reference of the key having been used for encryption in the ciphertext storing part.

16. (Currently amended) A plaintext detector system for analyzing potential susceptibility for blocks of plaintext, to be encrypted by an encryption algorithm, of being decrypted by an unauthorized party and increasing the security of the encryption of such plaintext, comprising:

a receiving unit [[for]] receiving a block of plaintext to be encrypted;

a counter unit connected to the receiving unit to separate, from the block of plaintext, a predetermined bit string, and to compute a value based on counting the predetermined bit string as virtually continuing bits to represent a susceptibility standard of unauthorized decryption; and

a detecting unit [[for]] comparing the computed value with a predetermined stored value wherein the block of plaintext is less than the susceptibility standard predetermined stored value is provided a first signal that will permit encryption and the block of plaintext that is equal or greater than the susceptibility standard predetermined

Art Unit: 2135

stored value is provided a second signal to change a manner of execution of the encryption algorithm of the block of plaintext to increase security.

17. (previously presented) The plaintext detector system of Claim 16 where the second signal enables a change of a key used by the encryption algorithm.

Allowable Subject Matter

1. The following is an examiner's statement of reasons for allowance: The prior art teaches counting the number of times the pseudorandom number key sequence has been utilized, but does not explicitly disclose counting specific bit values of the plaintext to suggest a condition that would render the overall encryption algorithm more susceptible to decryption attack.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

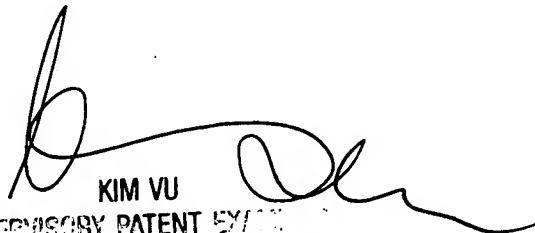
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
/RDM/

10/15/2007


KIM VU
SUPERVISORY PATENT EX/IN
TECHNOLOGY CENTER 2100